Return to Shelf

FR-9080

Naval Research Laboratory

Washington, DC 20375-5000

NRL Report 9080

Radar Waveforms Derived from Orthogonal Matrices

FRANK F. KRETSCHMER, JR. AND KARL GERLACH

Radar Division

February 14, 1989

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NRL Report 9080	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Research Laboratory 6b. OFFICE SYMBOL (*If applicable*) Code 5340	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (*City, State, and ZIP Code*) Washington, DC 20375-5000	7b. ADDRESS (*City, State, and ZIP Code*)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Chief of Naval Research 8b. OFFICE SYMBOL (*If applicable*) CNO	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*) Arlington, VA 22217-5000	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. 61153N; PROJECT NO. 021-05-43; TASK NO.; WORK UNIT ACCESSION NO. DN480-006

11. TITLE (*Include Security Classification*)
Radar Waveforms Derived from Orthogonal Matrices

12. PERSONAL AUTHOR(S)
Kretschmer, F. F., Jr., and Gerlach, Karl

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (*Year, Month, Day*)	15. PAGE COUNT
Interim	FROM _____ TO _____	1989 February 14	40

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB-GROUP	Waveforms, Coding, Pulse compression, Radar

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

In this report, new polyphase coded sequences are described that may be used to modulate a carrier frequency in pulse compression waveforms. These waveforms have low sidelobes when individual or multiple pulses are appropriately processed. They are related to orthogonal matrices that may be associated with complementary sequences and also with periodic waveforms having autocorrelation functions with constant zero-amplitude sidelobes. Periodic waveforms having zero sidelobes are of interest because of their relationship to complementary sequences and because the associated aperiodic waveform often has good properties. Also described in this report are sets of sequences whose cross-correlation functions sum to zero everywhere. A potential application is the elimination of ambiguous range stationary clutter.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Frank F. Kretschmer, Jr.	22b. TELEPHONE (*Include Area Code*) (202) 767-3599 22c. OFFICE SYMBOL 5340.1K

DD Form 1473, JUN 86 *Previous editions are obsolete.* SECURITY CLASSIFICATION OF THIS PAGE

S/N 0102-LF-014-6603

CONTENTS

RADAR WAVEFORMS DERIVED FROM ORTHOGONAL MATRICES

I. INTRODUCTION

Generally, modern radars incorporate pulse compression waveforms to simultaneously obtain sufficient energy on target for detection and the desired range resolution. This is achieved by coding a relatively long transmit waveform to achieve the bandwidth desired so that upon reception and matched filtering the pulse is compressed in time to a width that is approximately equal to the reciprocal of the bandwidth. The compressed pulse is equivalent to the autocorrelation of the transmit pulse in the absence of noise and Doppler shift. To not mask weak targets in the sidelobes of a stronger target, the sidelobes of the compressed pulse should be small.

Previous pulse compression waveforms are exemplified by the Frank, Barker, pseudo-random shift register codes, and the Lewis-Kretschmer polyphase codes [1]. In the present report we describe new pulse compression waveforms having low or zero sidelobes when an individual waveform or multiple dissimilar waveforms are processed. These waveforms, also referred to as coded sequences, are related to certain orthogonal matrices that are associated with complementary sequences and also periodic waveforms having constant amplitude autocorrelation sidelobes that are equal to zero. We also investigate periodic waveforms derived in a similar manner that have a constant sidelobe level equal to -1.

Complementary sequences are multiple code sequences having autocorrelation functions (ACFs) that sum to 0 everywhere except at the match point where the correlation peak occurs. New orthogonal processing is derived whereby the summed cross correlations of complementary sequences are identically equal to zero. Several codes of interest are shown to be able to remove a nonmoving ambiguous range target or clutter return. Also, subcomplementary sequences having ACFs that sum to 0 beyond a certain interval are described and the theory is generalized.

Periodic waveforms having a constant sidelobe level equal to 0 are related to complementary sequences; also, they are of interest because they have associated aperiodic waveforms that have low sidelobes. The relationship is developed between these periodic waveforms and circular Toeplitz matrices having inner products between the rows equal to 0. Closely related to these waveforms are those that are associated with circular Toeplitz matrices having inner products equal to -1. Several periodic and associated aperiodic codes are described that are based on Number Theory considerations that are established from the required inner products of the circular Toeplitz matrices. New codes are derived from the product of two periodic codes, and from a generalization of the Frank and the Lewis-Kretschmer P4 periodic codes; and also, it is shown that certain permutations of periodic codes having constant sidelobes of -1 or 0 are also periodic codes having the same property. In addition, a new class of periodic codes, referred to as reciprocal codes, are briefly described.

Manuscript approved May 2, 1988.

II. COMPLEMENTARY CODES

IIA. Basic Properties

Complementary sequences are coded sequences (complex numbers in general) having autocorrelation functions $G_i(k)$, which when time aligned and added together, sum to zero everywhere except at the match point. That is, by letting the ith sequence of length N and the jth unit amplitude element be denoted by $s_{i,j}$, the ith discrete autocorrelation is given by

$$G_i(k) = \begin{cases} \sum_{j=1}^{N-k} s^*_{i,j}\, s_{i,j+k} & 0 \le k \le N-1 \\ \sum_{j=1}^{N+k} s_{i,j} s^*_{i,j-k} & -(N-1) \le k < 0 \end{cases} \tag{1}$$

and for M sequences, the sum of the ACFs is given by

$$\sum_{i=1}^{M} G_i(k) = \begin{cases} 0 & k \neq 0, \\ NM, & k = 0 \end{cases} \tag{2}$$

where * represents complex conjugation and k denotes an integer offset from the match point at zero. It may be shown that at the match point the S/N ratio is maximized.

One of the early papers on complementary sequences by Golay [2] deals with pairs of binary coded sequences conceived in connection with an optical problem of multislit spectrometry. The formulation above allows for the more general case considered later where the elements of the sequences may be complex. Golay defines a set of complementary series as a pair of equally long binary sequences (consisting of ones and zeros) having the property that the number of pairs of like elements with a given separation in one series is equal to the number of pairs of unlike elements in the other series. Golay illustrates this with the two sequences (1001010001) and (1000000110) having three pairs of like and unlike adjacent elements, four pairs of like and unlike elements that are two elements apart, and so on. A later comprehensive paper by Tseng and Liu [3] describes generalized properties of complementary sets of binary sequences consisting of more than two sequences. Of particular interest in Ref. 3 are sets of subsequently described sequences referred to as mates that exhibit a certain kind of of orthogonality. In a later paper, Sivaswami [4] describes multiphase complementary sequences.

We now discuss basic matrix relationships that characterize complementary sequences. Let the rows of an $(M \times N)$ matrix S represent rows of M sequences, each of length N. That is,

$$S = \begin{bmatrix} S_1 \\ S_2 \\ \cdot \\ \cdot \\ \cdot \\ S_M \end{bmatrix} = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1N} \\ s_{21} & s_{22} & \cdots & s_{2N} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ s_{M1} & s_{M2} & \cdots & s_{MN} \end{bmatrix}. \tag{3}$$

The ACFs of each sequence using Eq. (1) may be written as

$$\begin{array}{lllll} G_1(k): & s_{11}s^*_{1N}, & s_{11}s^*_{1,N-1} & + s_{12}s^*_{1N}, & \cdots \\ G_2(k): & s_{21}x^*_{2N}, & s_{21}s^*_{2,N-1} & + s_{22}s^*_{2N}, & \cdot \\ \cdot & \cdot & \cdot & \cdot \quad \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \quad \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \quad \cdot & \cdot \\ G_M(k): & s_{M1}s^*_{MN}, & s_{M1}s^*_{M,N-1} & + s_{M2}s^*_{MN}, & \cdots \end{array} \tag{4}$$

from which it is observed that in order to satisfy Eq. (2) we require that the inner product of the first and last columns of Eq. (3) equal 0, the inner product of the first and $(n-1)$th columns plus the inner product of the second and nth columns equal 0, and so on. Letting $b(i)$ represent the ith column of Eq. (3), we can state the required conditions for complementary sequences as

$$Q(k) = \sum_{i=1}^{N-k} (b(i), b(i+k)) = 0, \qquad k = 1, 2, \cdots, N-1 \tag{5}$$

where (e, f) denotes the complex inner product of the vectors e and f given by

$$(e, f) = \sum_{i=1}^{M} e_i f_i^*.$$

From Eq. (5) it is noted that a sufficient condition for sequences to be complementary is that the columns of the S matrix in Eq. (3) be mutually orthogonal. As a simple example consider the (2×2) Hadamard matrix given by

$$H(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The ACFs of the first and second rows are $(1, 2, 1)$ and $(-1, 2, -1)$ respectively, which sum to $(0, 4, 0)$. Higher order Hadamard matrices having mutually orthogonal columns can be generated by the recurrence relation

$$H(k) = \begin{bmatrix} H(k-1) & H(k-1) \\ H(k-1) & -H(k-1) \end{bmatrix},$$

where $H(0) = 1$ and $H(1)$ is given by the example shown above. The next higher order Hadamard matrix $H(2)$ is given by

$$H(2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Tseng and Liu [3] describe methods for generating higher order complementary sequence matrices from any given complementary sequence matrix making use of orthogonal transformations.

Another binary complementary matrix can be generated from pseudorandom shift register codes [5]. Consider the simple three-element shift register code given by $(1, -1, -1)$. Forming a (4×4) matrix consisting of the (3×3) submatrix consisting of the code and its rotations, and a fourth row and column of 1's, we have

$$S = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

which has mutually orthogonal columns (and rows) and hence consists of complementary sequences.

Another example is given by the Frank [6] and the Lewis-Kretschmer [7] P4 code matrices. The Frank code matrix has elements that are the complex conjugates of the discrete Fourier transform (DFT) matrix. The $(N \times N)$ Frank code matrix F is given by

$$F = \begin{bmatrix} F_0 \\ F_1 \\ F_2 \\ \cdot \\ \cdot \\ \cdot \\ F_{N-1} \end{bmatrix} = \begin{bmatrix} W_N^0 & W_N^0 & W_N^0 & \cdots & W_N^0 \\ W_N^0 & W_N^1 & W_N^2 & \cdots & W_N^{N-1} \\ W_N^0 & W_N^2 & W_N^4 & \cdots & W_N^{2(N-1)} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ W_N^0 & W_N^{N-1} & W_N^{2(N-1)} & \cdots & W_N^{(N-1)(N-1)} \end{bmatrix}^*, \tag{6}$$

where $W_N = e^{-j2\pi/N}$ and $j = e^{j2\pi/4} = \sqrt{-1}$. For example, for $N = 4$, we have

$$F = \begin{bmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}, \tag{7}$$

which is to be seen to consist of mutually orthogonal columns and rows. The polyphase Frank code is formed by chaining or concatenating the successive rows of the F matrix. A Lewis-Kretschmer P4 code of length N^2 can also be written in terms of an orthogonal $(N \times N)$ matrix. The P4 code polyphase code elements are given by the phases [1,7]

$$\phi(i) = \frac{\pi}{P}(i - 1)^2 + \pi(i - 1), \quad i = 1, 2, \cdots, P \tag{8}$$

where P is the number of code elements. The Frank and P4 codes have several interesting properties that are later described in detail.

II-B. Additional Properties of Complementary Sequences of Particular Interest

We next discuss several additional properties that are related to different kinds of orthogonality.

1. Mates

First we discuss the concept of mates as defined by Tseng and Liu [3], consisting of two complementary sets of binary sequences.

Definition: A complementary set of sequences is said to be a mate of another set if the sum of the cross-correlation functions of the corresponding sequences in these two sets is zero everywhere.

From Ref. 3 we obtain the following theorem.

Theorem 1: Let $(S_1, S_2, \cdots S_p)$ *be a complementary set consisting of an even number of sequences where* S_1 *and* S_2, S_3 *and* S_4, $\cdots$, S_{p-1} *and* S_p *are pairs of sequences of the same length. Then*

$$[\tilde{S}_2, (-\tilde{S}_1), \tilde{S}_4, (-\tilde{S}_3), \cdots, \tilde{S}_p(-\tilde{S}_{p-1})]$$

is one of its mates (~ denotes a time reversal).

Proof: Let $C_{x\tilde{y}}$ denote the cross-correlation function between x and the time reversal of y. The theorem is proved from the fact that

$$C_{x\tilde{y}} + C_{y(-\tilde{x})} = C_{x\tilde{y}} + C_{(-x)\tilde{y}} = C_{x\tilde{y}} - C_{x\tilde{y}} = 0. \tag{9}$$

Note that the proof is based on the pairwise sum of the cross correlations of two sequences x and y with $\tilde{y}$ and $-\tilde{x}$, respectively. Actually this theorem is more general and is not restricted to complementary sets. As an example consider the two sequences S_1 and S_2 given by

$$(1, 1, 1, -1) \text{ and } (1, -1, -1, 1).$$

Their ACFs are

$$(-1, 0, 1, 4, 1, 0, -1) \text{ and } (1, 0, 1, 4, 1, 0, 1).$$

We next form the mate M_1 and M_2, which is given by

$$(1, -1, -1, 1) \text{ and } (1\ -1\ -1\ -1).$$

The cross correlation between (S_1, M_1) and (S_2, M_2) is

$$(-1, 2, 1, -2, -1, 0, 1) \text{ and } (1, -2, -1, 2, 1, 0, -1),$$

whose corresponding elements sum to zero. This is potentially useful in eliminating ambiguous range returns and for reducing mutual interference between radars operating in the same band.

2. *Cross Correlation Theorem*

Next, we derive a new orthogonality relationship which states that certain sets of complementary sequences have cross-correlation functions that sum to zero by using all pairwise permutations. Here, all cross-correlation function permutations are required in order that their sum be identically equal to zero. This differs from the concept of mates defined by Tseng and Liu whereby the sum of two cross correlations at a time is equal to zero. The cross-correlation theorem may be formally stated in the following theorem, which is proven in Appendix A.

Theorem 2: If the rows and columns of an $(N \times M)$ *matrix are orthogonal and all the columns except one sum to zero, then the sum of all cross correlations between nonidentical code words is zero.*

Examples of matrices satisfying the theorem are the circular shift register matrices having an appended row and column of 1's described previously and the Frank and P4 matrices.

3. *Orthogonality of Cross Correlation of Frank Code Matrix Rows*

A still different orthogonality relationship is presented as a subset of Theorem 2 that has potential applications in removing ambiguous range radar returns. Here, the cross correlations between codes, represented by the rows of a matrix with a given separation, sum to zero.

Theorem 3: Let the cross correlations between rows l *and* m *of an* $(N \times N)$ *Frank code matrix be represented by* $C_{lm}(n)$. *Then*

$$\sum_{l=0}^{N-1} C_{lm}(n) = 0, \quad n = 0, \pm 1, \pm 2, \ldots, \pm(N-1), \tag{10}$$

where $m \equiv (l + r) \bmod N$ *and* $r = 1, 2, \ldots, N-1$.

Proof: See Appendix B

As an example of removing a stationary target from the first ambiguous range interval, consider the simplified example illustrated in Fig. 1 for $N = 4$. First F_1, F_2, and F_3 of Eq. (7) are transmitted but not processed. Then F_0, F_1, F_2, and F_3 are transmitted, and during each sweep the return signals are processed with a filter matched to the most recent transmitted code. This is referred to as Channel 0 in Fig. 1. By summing the returns from the four sweeps beginning with F_0, ambiguous range targets (or clutter) from the first, second, and third ambiguous range intervals are eliminated according to the previous theorem. Moreover, since F_0, F_1, F_2, and F_3 are a complementary set of sequences, the sidelobes of stationary targets in the unambiguous range intervals sum to zero. Other processing channels may be included as indicated in Fig. 1, if desired, which are matched to the other range intervals, and stationary clutter from the mismatched range intervals is eliminated. While the theorem has been shown to apply to the Frank code matrix, it has been found to also be true for the Lewis-Kretschmer P1, P3, and P4 code square matrices, and also the P2 code matrix for odd square integers only (see Ref. 1 for a description of the P1, P2, and P3 polyphase codes).

4. *Subcomplementary Sequences*

Another concept of interest is that of subcomplementary sequences [8]. These consist of a pair of sequences of length $2^k \tau_0$ $(k = 1, 2, \cdots)$ having ACFs that sum to zero for all shifts equal to or greater than the ACF duration τ_0 of an underlying waveform.

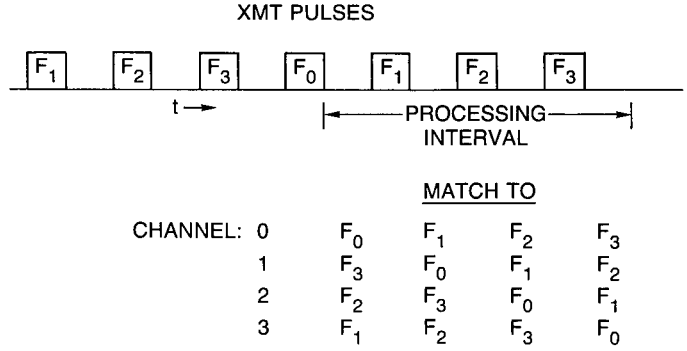


Fig. 1 — Example of processing to remove stationary clutter and resolve range ambiguity

For a signal S_0 consisting of N elements and having an ACF duration of $\pm\tau_0$, Sivaswami [8] shows that the $2N$ sequence S_1 formed by concatenating S_0 with itself, (S_0S_0) and the $2N$ sequence $\hat{S}_1$ formed by concatenating S_0 with S_0 phase reversed $[S_0\,(-S_0)]$ have ACFs that when summed have zero time sidelobes outside $\pm\tau_0$. Also, the resulting ACF amplitude is four times the ACF of the sequence S_0. The procedure described above may be repeated so that the new pair of sequences $S_2 = [S_1S_1]$ and $\hat{S}_2 = [S_1(-S_1)]$ are four times as long as S_0 and hence have four times the energy. The summed ACFs are then equal to eight times the ACF of S_0. The general term given by Sivaswami [8] is $S_m = [S_{m-1}S_{m-1}]$ and $\hat{S}_m = [S_{m-1}(-S_{m-1})]$. Any coded signal having desirable properties, such as the chirp, Barker, shift register, and polyphase codes [1] may be used for S_0. As an example let $S_0 = (1, 1, 1, -1)$; then

$$S_1 = (1, 1, 1, -1, 1, 1, 1, -1)$$

$$\hat{S}_1 = (1, 1, 1, -1, -1, -1, -1, 1).$$

The ACF of S_0 is

$$(-1, 0, 1, 4, 1, 0, -1),$$

the ACF of S_1 is

$$(-1, 0, 1, 4, -1, 0, 1, 8, 1, 0, -1, 4, 1, 0, -1),$$

and the ACF of $\hat{S}_1$ is

$$(1, 0, -1, -4, -3, 0, 3, 8, 3, 0, -3, -4, -1, 0, 1).$$

Summing the ACFs of S_1 and $\hat{S}_1$ we have

$$(0, 0, 0, 0, -4, 0, 4, 16, 4, 0, -4, 0, 0, 0, 0),$$

which is equal to 4 times the ACF of S_0.

We generalize the concept of subcomplementary sequences by the following theorem.

Theorem 4: For any coded sequence S_0 a subcomplementary set of sequences results from the Kronecker product of S_0 and a matrix consisting of a set of complementary sequences.

Proof: See Appendix C.

The matrix in Theorem 4 is more general than the underlying matrix that is related to the recursive relation given in Ref. 8, which consists of two rows of binary elements. The matrix in Theorem 4 can be any complementary matrix such as the Frank or P4 code matrices, and the shift register code matrix previously discussed.

III. PERFECT PERIODIC AND ASSOCIATED APERIODIC CODES

The investigation of periodic codes is motivated by their relationship to complementary codes, by their orthogonal properties, and by the fact that many good aperiodic codes are derived from periodic codes having low sidelobe levels. This is exemplified by the constant amplitude periodic Frank code [9], which has a constant sidelobe level of 0, referred to here as a perfect periodic code (PPC). We show in this section that the Lewis-Kretschmer P4 code and the generalized Frank and P4 codes also have zero periodic sidelobes, and moreover the amplitude of the aperiodic P4 code ACF is invariant with rotation. Doppler properties of a PPC are compared with the corresponding aperiodic code. Also a new PPC is described that is formed from the product of two PPCs. Relationships are derived between PPCs of length N^2 and an $N \times N$ orthogonal code matrix.

Figure 2 shows a periodic waveform consisting of concatenated, constant amplitude, aperiodic codes that are digitally coded. The complex values of $a_0, a_1, \cdots, a_{N-1}$ make up the code word of length N in a given pulse repetition interval (PRI). This code word is repeated in succeeding PRIs.

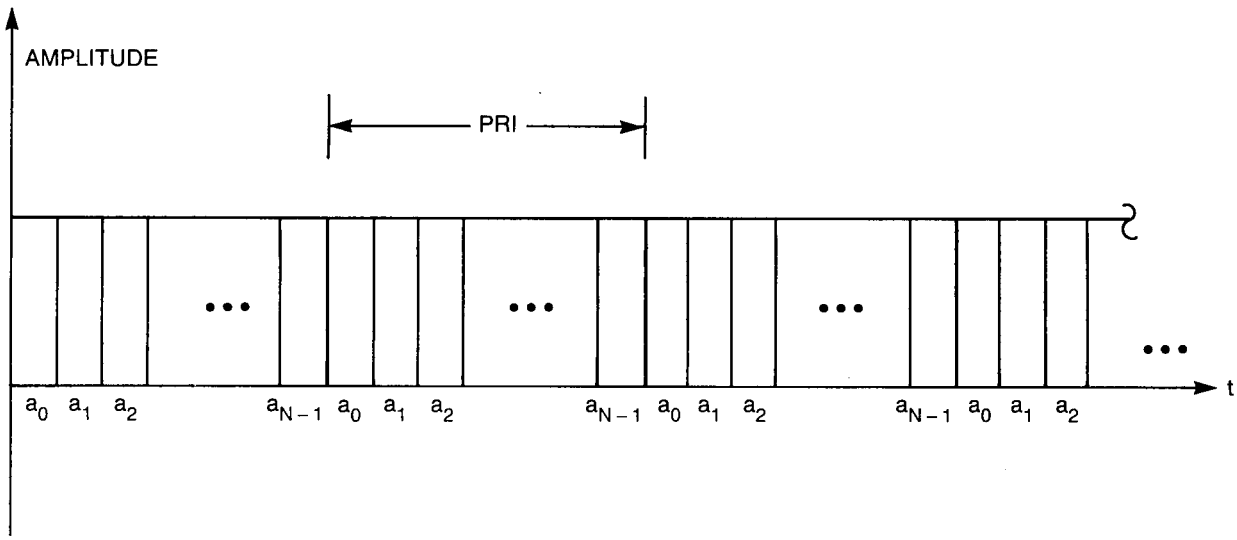


Fig. 2 — Digitally encoded periodic waveform

A PPC is defined to be a periodic code whose ACF has zero sidelobes and whose amplitude is uniform (maximum power efficiency = 1), i.e., $|a_1| = |a_2| = \cdots = |a_{N-1}|$. An asymptotically PPC has the property that as $N \to \infty$ the code's ACF has zero relative sidelobes and its power efficiency is one.

III-A. Properties of Periodic Waveforms

We define a code word **a** such that **a** is a row vector of length N and

$$\mathbf{a} = (a_0, a_1, a_2, \cdots, a_{N-1}), \tag{11}$$

where a_n, $n = 0, 1, 2, \cdots, N-1$ are the elements of the code word. A periodic code is one that repeats the code word **a** indefinitely. Hence if $\mathbf{a}_{pc}$ is the periodic code associated with **a**, then

$$\mathbf{a}_{pc} = \mathbf{a} \circ \mathbf{a} \circ \mathbf{a} \cdots, \tag{12}$$

where the symbol $\circ$ denotes concatenation.

On reception, a periodic code is match filtered with its periodic code word. The output of the correlation process is also periodic with a period, N. Hence, the matched response repeats every N unit time delays as does the sidelobe response.

We form an $N \times N$ circulant matrix A, based on each of the possible unit time delays of the received code:

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \cdots & a_{N-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}. \tag{13}$$

Note that the inner product between the 1st row and the $m+1$th row, $m = 0, 1, \cdots, N-1$ is equal to the output of the correlation process at the mth unit time delay of any period. Also the inner product of the m_1th row and the m_2th row is equal to the inner product of the m_3th and m_4th row if $m_1 - m_2 = m_3 - m_4$. In fact if we denote r_m to be the inner product of the 1st and $m+1$th rows, then

$$AA^t = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{N-1} \\ r_1^* & r_0 & r_1 & \cdots & r_{N-2} \\ r_2^* & r_1^* & r_0 & \cdots & r_{N-3} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ r_{N-1}^* & r_{N-2}^* & r_{N-3}^* & \cdots & r_0 \end{bmatrix}, \tag{14}$$

where t denotes the matrix conjugate transpose. Here the diagonal elements are identical and equal to the matched response, and the off-diagonal elements are associated with the $N-1$ sidelobe responses.

We constrain the code word **a** such that

$$|\mathbf{a}|^2 = N, \tag{15}$$

where $|\cdot|$ denotes the vector magnitude. We call a periodic code "perfect" if all the code elements have equal magnitude and all of the sidelobe responses are zero. The first condition implies the code is 100% power efficient or

$$|a_n|^2 = 1, \quad n = 0, 1, 2, \cdots, N-1. \tag{16}$$

Zero sidelobe response implies that

$$AA^t = NI, \tag{17}$$

where I is the $N \times N$ identity matrix.

Equation (17) indicates that the A matrix consists of orthogonal rows, and for a circulant matrix this implies that the columns are also orthogonal and hence the A matrix also consists of a set of complementary sequences. Thus complementary sequences can be generated from the circulant matrix of the Frank code and other codes that are discussed in a later section, and also from the Frank code matrix previously described.

III-B. P4 Code

In Appendix D, it is shown that the Lewis-Kretschmer P4 code has a periodic ACF with 0 sidelobes.

1. Properties of P4 Aperiodic Code

We have shown that the P4 code, like the Frank code, is a PPC. The P4 polyphase code was originally derived by sampling the phases of chirp signal and, like the chirp signal, it has good Doppler properties and low sidelobes. Figure 3 shows a 100-element P4 code ACF for zero Doppler. Figure 4 shows the ambiguity surface for the same code. The output of a receiver matched to a P4 code is represented by Fig. 4 for any given Doppler shifted return signal. Thus, the cut along the zero Doppler axis corresponds to the ACF shown in Fig. 3. A Doppler shifted return signal causes a mismatch thereby changing the filtered signal as shown by the ambiguity diagram. The time delay axis is normalized to the uncompressed pulsewidth, and the sample numbers along the delay axis correspond to range cells. The Doppler axis of the ambiguity function is given in terms of the product of the Doppler frequency and the uncompressed pulse duration. A value of unity corresponds to a 2π phase shift due to Doppler across the uncompressed pulse. The matched filter output for complex discrete time samples taken once per code element may be stated mathematically as

$$e(k) = \begin{cases} \sum_{i=1}^{N-k} c^*(i)c(i+k)\, e^{j(i-1+k)\Delta} & 0 \le k \le N-1 \\ \sum_{i=1}^{N+k} c(i)c^*(i-k)e^{j(i-1)\Delta} & -(N-1) \le k < 0 \end{cases} \tag{18}$$

where

c_i is the ith code element,
k is the time delay index relative to match point, and
$\Delta = 2\pi f_d \tau$ (Doppler phase shift in sampling internal τ).

The ambiguity function is given by the squared amplitude of $e(k)$. The ambiguity function of the P4 code is similar to that of the Frank code, which is shown in Refs. 1 and 7 to be derivable from the sampled phases of a step-chirp waveform.

2. Invariance of Rotated P4

While any of the PPCs remain PPCs if the underlying aperiodic code is circularly rotated, it is not true in general that aperiodic codes have ACF amplitudes that are invariant with circular rotation of the code word. However, in Appendix E we prove that the P4 code has this invariance property.

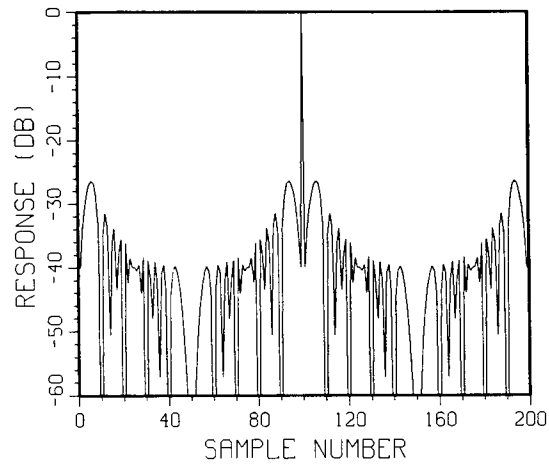


Fig. 3 — 100 element P4 code ACF

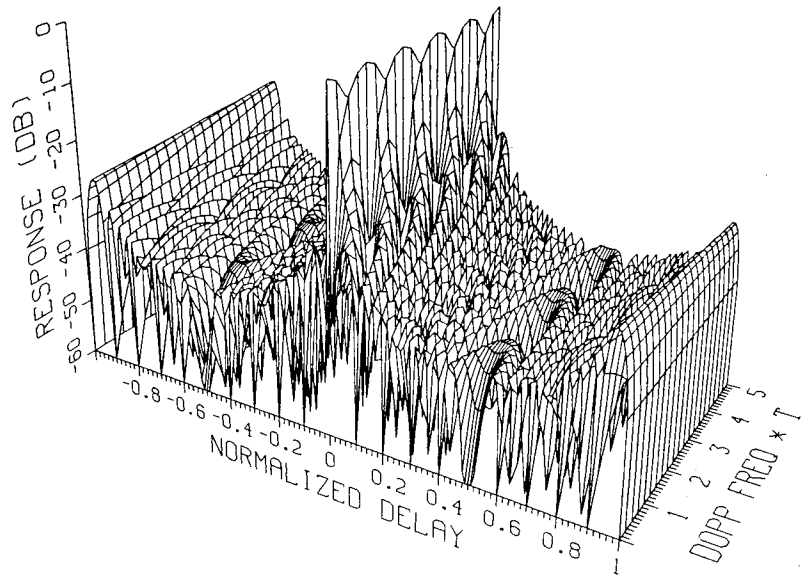


Fig. 4 — 100 element P4 code ambiguity function

III-C. Doppler Properties of a Periodic Frank Code

Doppler properties of a periodic Frank code were investigated to determine the effect on the zero sidelobe level achieved under zero Doppler conditions. This was done on a computer by considering two concatenated Frank codes as shown in Fig. 5 as the return signal having a specified Doppler frequency f_d. The radar receiver complex video signal was assumed to be matched over one code length T to a zero-Doppler received Frank code, and the resultant computer plots were obtained by performing the convolution indicated in Fig. 5. Hence, we can show on each plot the resultant aperiodic and periodic sidelobes and peaks. In Fig. 6 the aperiodic sidelobes are shown to the right and left of the peaks, and the periodic sidelobes are shown between the two peaks. It was found that the peak sidelobe levels of the aperiodic and periodic ACFs are nearly the same for Doppler shifts of 0.375 and above.

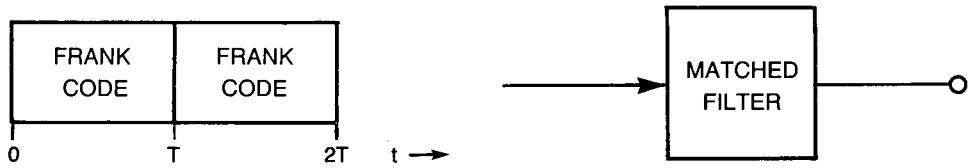


Fig. 5 — Determination of aperiodic and periodic sidelobes of a 100-element Frank code

III-D. Relationship Between Orthogonal N × N Matrices and Perfect Periodic Codes of Length N^2

We address here the question of what the properties of an $N \times N$ matrix must be in order to be able to concatenate the rows of this matrix to form a code of length N^2, which when periodically repeated is a perfect periodic code. The sufficient conditions for this to apply are stated in the following Theorem.

Theorem 5: Consider an $N \times N$ matrix E with elements on the unit circle. Let E have mutually orthogonal rows. In addition, let all rotations of any two columns of E be mutually orthogonal. Then a perfect periodic code results from concatenating the rows of E.

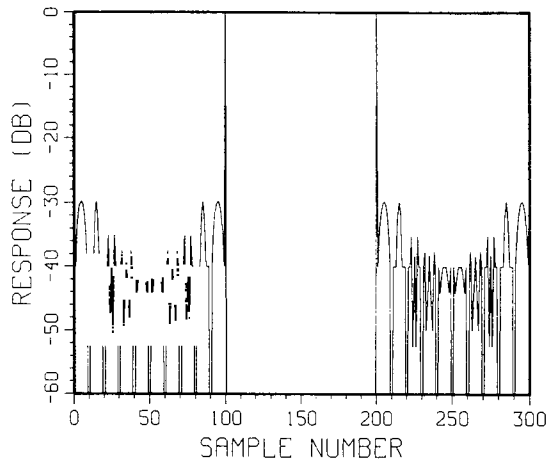
Proof: See Appendix F.

Note that any $N \times N$ matrix satisfying the conditions of Theorem 5 also has rows corresponding to a set of complementary sequences.

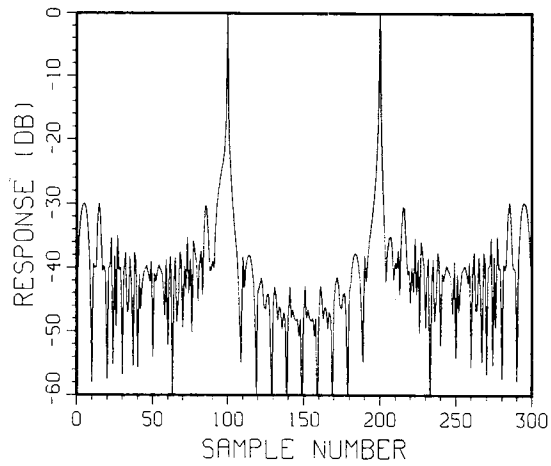
III-E. New Periodic Codes

1. Generalized Frank and P4 codes

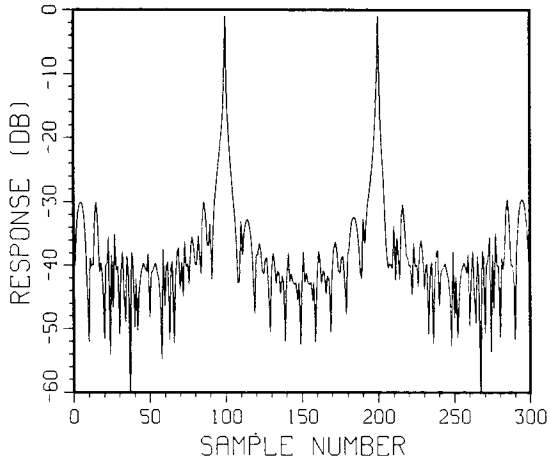
From the previous section we can generate new PPCs that we call generalized Frank codes by postmultiplying the Frank code matrix by a diagonal matrix D consisting of the elements $(d_0, d_1, d_2 \cdots, d_{N-1})$. This has the effect of multiplying each element in column 1 of Eq. (6) by d_0, in column 2 by d_1, and so on. Since the Frank code matrix meets the conditions of Theorem 5, and these conditions are not affected by the matrix D, we see that the resultant $N \times N$ matrix corresponds to a PPC. Also, it has been found by computer simulation that a P4 code of length N^2 can be written in terms of an $N \times N$ matrix satisfying Theorem 5 and we can then generate, in a similar manner to that described above, a generalized P4 code that retains the properties of being a PPC.



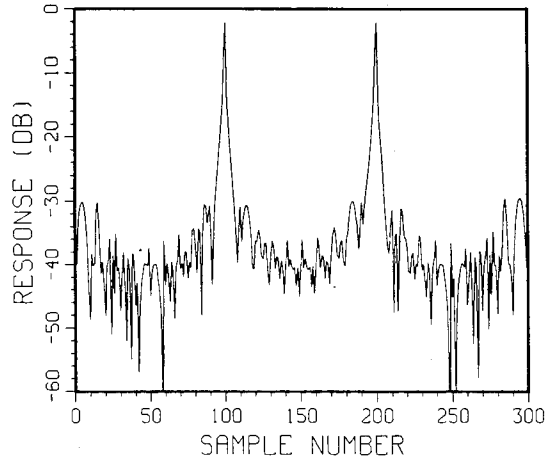
(a) $f_d T = 0$



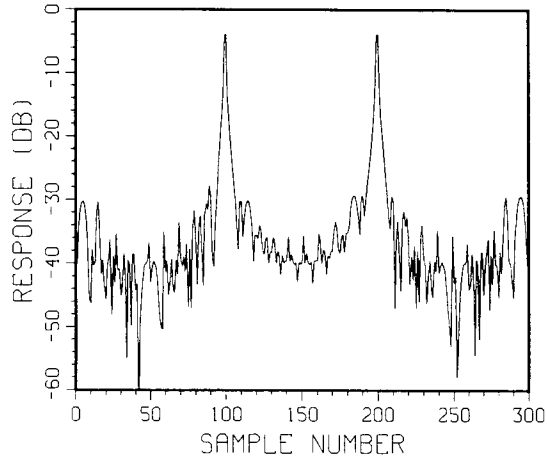
(b) $f_d T = 0.125$



(c) $f_d T = 0.25$



(d) $f_d T = 0.375$



(e) $f_d T = 0.5$

Fig. 6 — Aperiodic and periodic components of a 100-element Frank code

2. Frank—Lewis-Kretschmer P4 Product Code

Another new PPC may be generated by forming the product, code element by code element, of odd length Frank and P4 codes. This is proved in Appendix G.

3. Permutation Codes

Appendix H shows that if $a(n)$, $n = 0, 1, 2, \ldots N-1$ is a code having 0 or -1 periodic sidelobes, then $a_{Mn \bmod N}$, $n = 0, 1, \ldots N-1$, where M is an integer that is relatively prime to N, also has the same periodic sidelobes.

$$\begin{aligned}
\text{Ex: Let } \mathbf{a} &= a_0\ a_1\ a_2\ a_3\ a_4 \\
\text{Code 1} &= a_0\ a_2\ a_4\ a_1\ a_3\ , \quad M = 2 \\
\text{Code 2} &= a_0\ a_3\ a_1\ a_4\ a_2\ , \quad M = 3 \\
\text{Code 3} &= a_0\ a_4\ a_3\ a_2\ a_1\ , \quad M = 4
\end{aligned}$$

Codes 1, 2 and 3 have the same -1 or 0 periodic sidelobes as **a**.

4. Reciprocal Codes

In a companion report written by the authors [10], a new class of codes is derived that is referred to as reciprocal codes. They are based on the fact that any circulant matrix A as given by Eq. (13) may be written in terms of its eigenvectors and eigenvalues as

$$A = B\ \Lambda\ B^*, \tag{19}$$

where B is a Butler matrix (discrete Fourier transform matrix) of eigenvectors of A and Λ is a diagonal matrix of eigenvalues of A. Thus all circulant matrices have the same eigenvectors and differ only in their eigenvalues. Reference 10 shows that as a consequence of Eq. (19), a PPC word may be multiplied by B to generate another PPC word that consists of the eigenvalues of the A matrix of the original word.

IV. ASYMPTOTIC PERFECT PERIODIC CODES AND THEIR APERIODIC PROPERTIES

An asymptotic perfect periodic code (APPC) is a periodic code that becomes perfect as the number of code elements, N, in the periodic code word approaches infinity. For finite N either the sidelobe level is nonzero and/or the power efficiency is less than 100% for these codes. However, as $N \to \infty$, either the sidelobe level is zero or approaches zero and/or the power efficiency is 100% or approaches 100%.

Examples of codes that are APPCs are the shift register code, the primitive root code, the quadratic residue code, and the index code. All of these codes, except the index code, are assumed to have a subpulse amplitude of unity, and have a sidelobe level (voltage) equal to -1 for all time delays. (Note that for an N-element code the peak or match point is assumed to be N). The index code's first element is equal to zero, and the remaining unit amplitude elements are polyphase.

Letting ϵ equal the constant sidelobe level of a given APPC, we have by similar arguments to Eqs. (11) through (16) that

$$AA^t = \begin{bmatrix} N & \epsilon & \cdots & \epsilon \\ \epsilon & N & \cdots & \epsilon \\ \cdot & & \cdot & \\ \cdot & & \cdot & \\ \cdot & & \cdot & \\ \epsilon & \epsilon & \cdots & N \end{bmatrix}. \tag{20}$$

The APPCs described above must satisfy condition (20). In this section we describe these codes and also show the associated aperiodic autocorrelation and ambiguity functions. Costas sequences are also described because they are related to primitive root codes. We also show that the cross correlation between different primitive root codes of the same length have sidelobes that are down by approximately the time bandwidth product of the code, or equivalently, the pulse compression ratio, which is determined by the number of code elements.

IV-A. Shift Register Codes

These codes, also known as pseudorandom shift register codes, when periodically repeated are known to have a periodic ACF whose sidelobes are a constant equal to -1. These codes have been studied extensively and are described in Refs. 9, 10, and 11.

IV-B. Primitive Root Code

The N code words of the primitive root code [12] are defined as

$$a_n = W_{N+1}^{\alpha^n}, \qquad n = 0, 1, 2, \cdots, N-1$$

where $N-1$ must be a prime number and α is a primitive root modulo $N+1$ [12]. Example plots of the aperiodic ACF of the primitive root code and its ambiguity function are given in Figs. 7 and 8, respectively, for $N = 100$ and $\alpha = 2$ ($N + 1 = 101$ is a prime number).

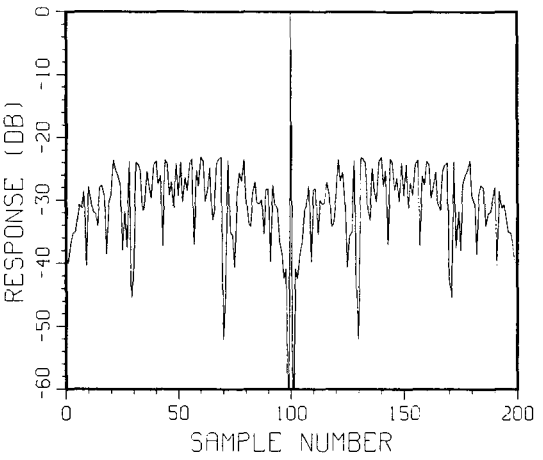


Fig. 7 — ACF of primitive root code ($p = 101$, $\alpha = 2$)

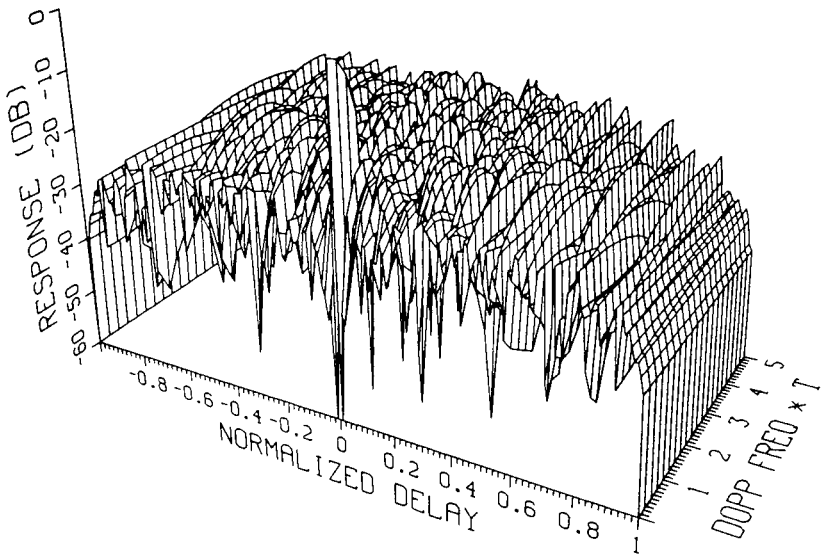


Fig. 8 — Ambiguity function of the primitive root code (p = 101, α = 2)

A different 101-element primitive root code (α = 3) is shown in Fig. 9, and the cross correlation function (CCF) between the two primitive root codes is shown in Fig. 10. These results are typical for the cross correlations between two primitive root codes of the same length or number of elements; the sidelobes are down from the peak by approximately the pulse compression ratio.

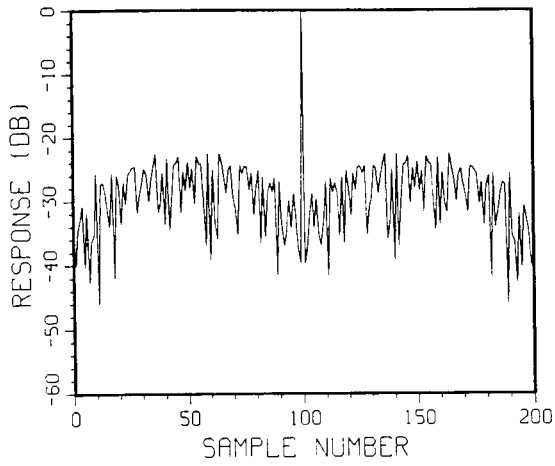


Fig. 9 — ACF of the primitive root code (p = 101, α = 3)

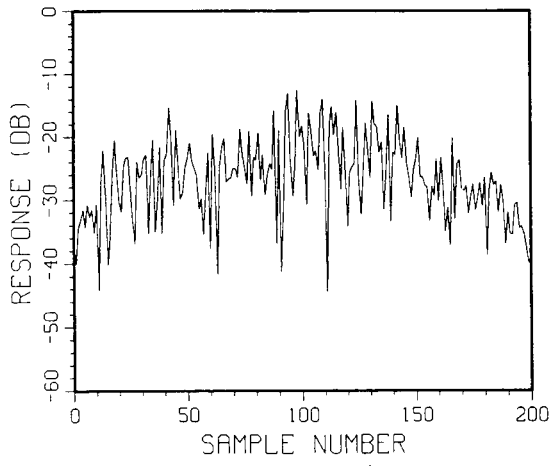


Fig. 10 — CCF of primitive root codes (p 101, α = 2) and (p = 101, α = 3)

A related subject that has received recent attention in the literature is Costas arrays [13,14]. This consists of reordering the tones of a step-chirp waveform in order to eliminate the range-Doppler coupling associated with the waveform, and also to prevent any large peaks in the sidelobe region of the ambiguity function. The Costas array ordering of the tones assumes that no more than one tone will simultaneously correlate with itself over all delays and Doppler frequencies in the pedestal region of the ambiguity function.

For a given number of tones N, the tones are ordered according to the sequence

$$\alpha^0, \alpha^1, \cdots \alpha^{N-1} \quad \text{mod } (N + 1),$$

where α is the primitive root of $N + 1$. An example of an ACF and ambiguity function for a Costas array is shown in Figs. 11 and 12 for $N = 10$ and $\alpha = 7$.

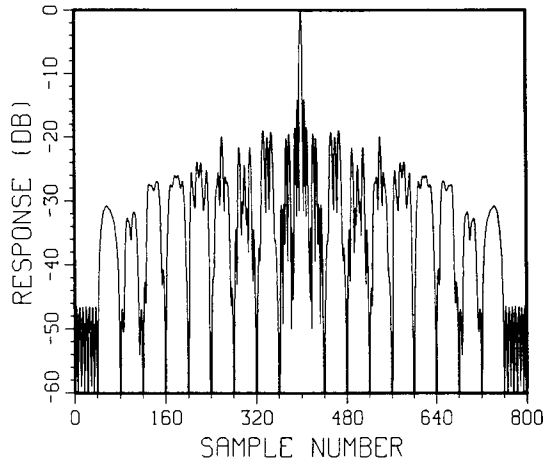


Fig. 11 — ACF of Costas sequence
($p = 11$, $\alpha = 7$)

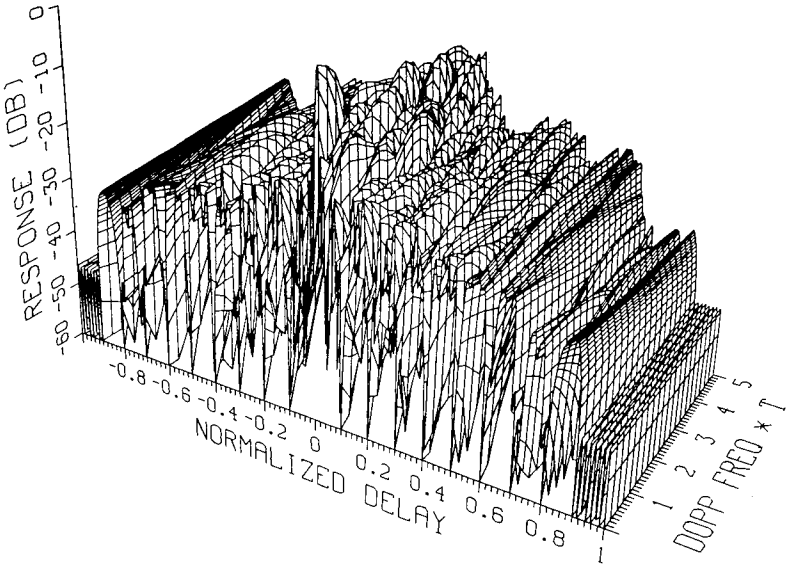


Fig. 12 — Ambiguity function of Costas sequence
($p = 11$, $\alpha = 7$)

IV-C. Quadratic Residue Code

For this binary code, we introduce the Legendre symbol [12]: (q/p). This symbol is defined for all q that are not divisible by p; it is equal to 1 if q is a quadratic residue of p and is equal to -1 otherwise. Note that q is a quadratic residue of p if the congruence

$$z^2 = q \text{ mod } p$$

has a solution.

With these preliminaries the code is defined as

$$a_n = (n/N), \quad n = 0, 1, \cdots, N - 1$$

where N is prime number of the form $4m - 1$. Note that we define $(0/N) = 1$. For example for $N = 11$, the code word **a** is given by

$$\mathbf{a} = (1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1,).$$

Plots of the aperiodic ACF and the ambiguity function are shown in Figs. 13 and 14 respectively.

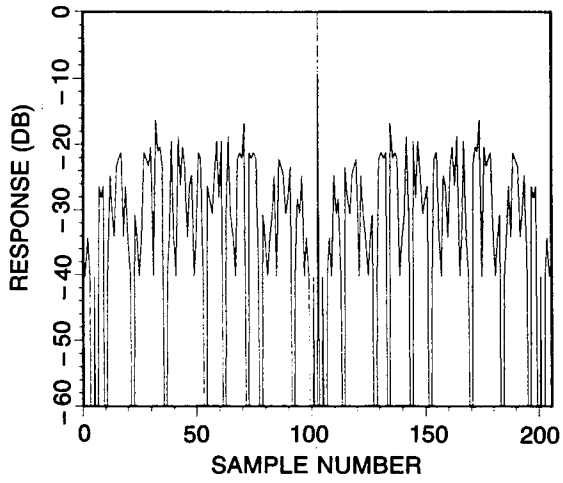


Fig. 13 — Aperiodic ACF of the quadratic residual code, $p = 103$

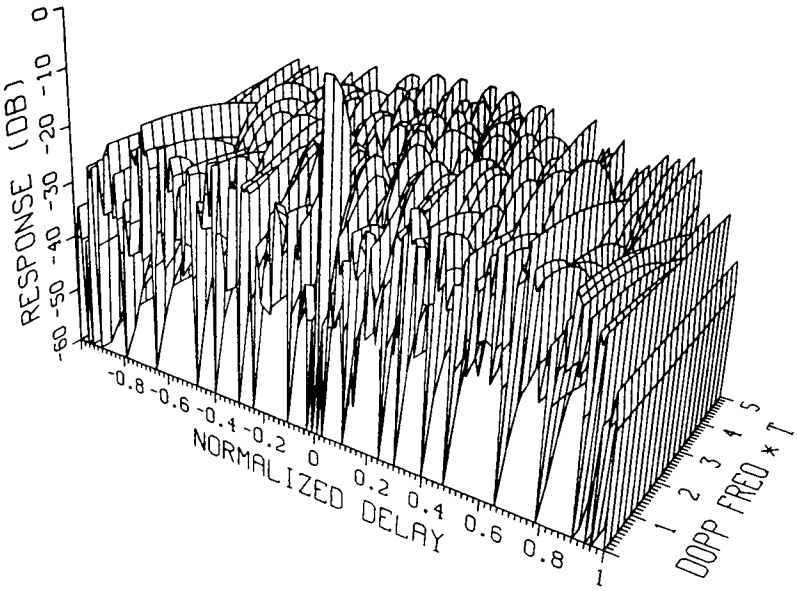


Fig. 14 — Ambiguity function of the quadratic residue code, $p = 103$

IV-D. Index Codes

Let N be an odd prime and α be a primitive root of N, i.e., $\{\alpha^0, \alpha^1, \cdots, \alpha^{N-2}\}$ mod N maps into $\{1, 2, \cdots, N-1\}$. If

$$\alpha^x \equiv y \bmod N,$$

then x is defined as the index of y modulo N to the base α, or

$$x = \mathrm{ind}_\alpha y.$$

In fact for every $y \in \{1, 2, \cdots, N-1\}$ there is an associated index $x \in \{0, 1, \cdots, N-2\}$.

For example for $N = 5$, 2 is a primitive root and

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3 \bmod 5.$$

Hence

$$\mathrm{ind}_2\, 1 = 0,\ \ \mathrm{ind}_2\, 2 = 1,\ \ \mathrm{ind}_2\, 3 = 3,\ \ \mathrm{ind}_2\, 4 = 2.$$

With these mathematical preliminaries, the code is defined as (see Appendix I for derivation)

$$a_n = W_{N-1}^{\mathrm{ind}_\alpha n}, \quad n = 0, 1, 2, \cdots, N-1$$

where N is a prime number and

$$W_{N-1}^{\mathrm{ind}_\alpha 0} \equiv 0.$$

Plots of the aperiodic ACF of the index code and its ambiguity function are given in Figs. 15 and 16 for $N = 101$ and $\alpha = 3$.

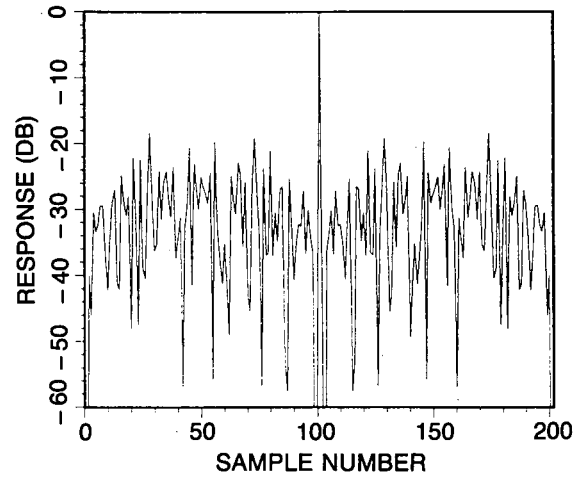


Fig. 15 — ACF of index code (101, 3)

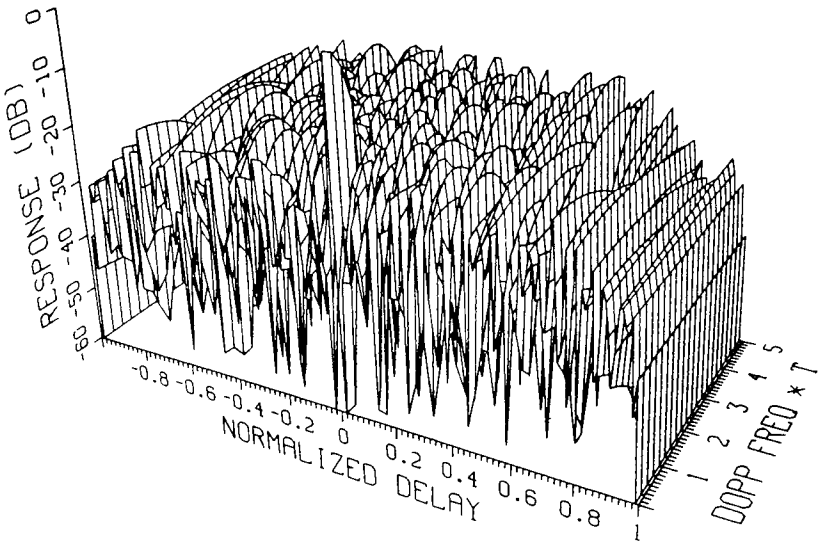


Fig. 16 — Ambiguity function of the index code (101, 3)

V. SUMMARY

In this report, we have described new pulse compression waveform coding on individual and multiple dissimilar pulses that result in low sidelobes after processing. Low sidelobes are important in radar applications in order that small targets are not masked in the sidelobes of nearby strong targets. Also, orthogonal waveforms have been found that have cross correlations that sum to zero everywhere. This has potential applications in resolving ambiguous range targets and in removing ambiguous range clutter in medium- or high-PRF radars.

In particular, we have extended the theory of complementary sequences, and periodic waveforms having ACFs, or compressed waveforms, with 0 or -1 sidelobe levels. Complementary sequences may be regarded as the coding modulation that is applied to multiple radar waveforms. The complementary property signifies that the sum of the individually compressed pulses has 0 sidelobes. Periodic coded waveforms having 0 or -1 sidelobe ACFs are of interest because the associated periodic coded waveforms often have low sidelobes and, for the 0 sidelobe case, do not degrade significantly in the presence of mismatches caused by Doppler-shifted return signals.

By extending the theory of complementary sequences and periodic waveforms having 0 or -1 sidelobes, new classes of waveforms have been found that have low sidelobes. Theorems have been derived that extend the existing theory and that show new relationships between complementary sequences and periodic waveforms having 0 sidelobes. Also, multiple orthogonal coded waveforms have been found that have cross correlation functions that sum to zero.

VI. ACKNOWLEDGMENT

The assistance of F. C. Lin is gratefully acknowledged.

VII. REFERENCES

1. B.L. Lewis, F.F. Kretschmer, Jr., and W.W. Shelton, *Aspects of Radar Signal Processing* (Artech House Inc., Norwood, MA, 1986).

2. M.J.E. Golay, "Complementary Series," *IRE Trans. Inf. Theory* **IT-7**, 82-87 (1961).

3. C.C. Tseng and C.L. Liu, "Complementary Sets of Sequences," *IEEE Trans. Inf. Theory* **IT-18**(5), 644-651 (1972).

4. R. Sivaswami, "Multiphase Complementary Codes," *IEEE Trans. Inf. Theory* **IT-24**(5), 546-552 (1978).

5. G. Weathers and E.M. Holiday, "Group-Complementary Array Coding for Radar Clutter Rejection," *IEEE Trans. Aerosp. Electron. Syst.* **AES-19**(3), 369-379 (1983).

6. R.L. Frank, "Polyphase Codes with Good Nonperiodic Correlation Properties," *IEEE Trans. Inf. Theory* **IT-9**, 43-45 (1963).

7. F.F. Kretschmer, Jr. and B.L. Lewis, "Doppler Properties of Polyphase Coded Pulse Compression Waveforms," *IEEE Trans. Aerosp. Electron. Syst.* **AES-19**(4), 521-531 (1983).

8. R. Sivaswami, "Digital and Analog Subcomplementary Sequences for Pulse Compression," *IEEE Trans. Aerosp. Electron. Syst.* **AES-14**(2), 343-350 (1978).

9. F.E. Nathanson, *Radar Design Principles* (McGraw-Hill Book Co., New York, (1969).

10. Karl Gerlach and F.F. Kretschmer, Jr., "Reciprocal Perfect and Asymptotically Perfect Periodic Radar Waveforms and Their Aperiodic Properties," NRL Report 9059 (in publication).

11. S.W. Golomb, *Shift Register Sequences* (Holden-Day, Inc., San Francisco, 1967).

12. M.R. Schroeder, *Number Theory in Science and Communication* (Springer-Verlag, 1986), 2nd edition.

13. J.P. Costas, "A Study of a Class of Detection Waveform Having Nearly Ideal Range-Doppler Ambiguity Properties," *Proc. IEEE* **72**(8), 996-1009 (1964).

14. S.W. Golomb and H. Taylor, "Construction and Properties of Costas Arrays," *Proc. IEEE* **72**(9), 1143-1163 (1964).

Appendix A

CROSS CORRELATION THEOREM

We define N code words with M elements each as

$$\mathbf{a}_n = (a_{11}, a_{12}, \cdots, a_{1M}), \quad n = 1, 2, \cdots, N. \tag{A1}$$

We arrange these code words to be the rows of the following $N \times M$ matrix:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1M} \\ a_{21} & a_{22} & \cdots & a_{2M} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{N1} & a_{N2} & \cdots & a_{NM} \end{bmatrix}. \tag{A2}$$

We show that

Cross Correlation Theorem: If the rows and columns of A are orthogonal and all columns except one sum to zero, then the sum at all cross correlations between nonidentical code words is zero.

Proof: A correlation vector of length $2M - 1$ between code words is defined as

$$\mathbf{c}_{mn} = \mathbf{a}_m * \tilde{\mathbf{a}}_n, \quad m, n = 1, 2, \cdots, N \tag{A3}$$

where $*$ denotes linear convolution and $\sim$ denotes the time-reversed complex conjugate of $\mathbf{a}_n$. The center element of c_{mn} is called the match point. This point can be computed by taking the inner products between the rows of A. However, since the rows are orthogonal, the contributions from the cross correlations ($m \neq n$) to the match point is zero. Hence

$$\text{Match Point} \left\{ \sum_{\substack{m,n=1 \\ m \neq n}}^{N} \mathbf{c}_{mn} \right\} = 0. \tag{A4}$$

If the columns are orthogonal, it is known that the codes are complementary or that

$$\text{Sidelobes} \left\{ \sum_{n=1}^{N} \mathbf{c}_{nn} \right\} = 0, \tag{A5}$$

i.e., the sum of the autocorrelation vectors is zero everywhere except the match point. Thus

$$\text{Sidelobes}\left\{\sum_{\substack{m,n=1\\ m\neq n}}^{N}\mathbf{c}_{mn}\right\} = \text{Sidelobes}\left\{\sum_{\substack{m,n=1\\ m\neq n}}^{N}\mathbf{c}_{mn} + \sum_{n=1}^{N}\mathbf{c}_{mn}\right\} \tag{A6}$$

$$= \text{Sidelobes}\left\{\sum_{m,n=1}^{N}\mathbf{a}_m * \tilde{\mathbf{a}}_n\right\}$$

$$= \text{Sidelobes}\left\{\left(\sum_{n=1}^{N}\mathbf{a}_n\right) * \left(\sum_{n=1}^{N}\tilde{\mathbf{a}}_n\right)\right\}.$$

If the columns of A sum to zero everywhere except in one position (say the kth), then

$$\sum_{n=1}^{N}\mathbf{a}_n = (0, 0, \cdots, 0, \alpha_k, 0, \cdots, 0) \triangleq \mathbf{b}, \tag{A7}$$

where α_k is the sum in the kth position. It is straightforward to show that

$$\text{Sidelobes}\{\mathbf{b} * \tilde{\mathbf{b}}\} = 0. \tag{A8}$$

Combining Eqs. (A4) and (A8), the theorem follows.

Appendix B

PROOF OF THEOREM 3

Theorem 3: Let the cross correlations between rows l and m of an $(N \times N)$ Frank code matrix be represented by $C_{lm}(n)$. Then

$$\sum_{l=0}^{N-1} C_{lm}(n) = 0, \qquad n = 0, \pm 1, \pm 2, \ldots, \pm(N-1)$$

where $m \equiv (l + r)$ mod N and $r = 1, 2, \ldots, (N - 1)$.

Proof: The cross correlation function of the two complex sequences $x(k)$ and $y(k)$, each of length N, is given by

$$\begin{aligned} C_{lm}(n) &= \sum_{k=0}^{N+n-1} x(k)y^*(k - n), \qquad \text{for} \quad n \leq 0, \\ C_{lm}(n) &= \sum_{k=0}^{N-n-1} x(k + n)y^*(k), \qquad \text{for} \quad n > 0. \end{aligned} \tag{B1}$$

Let $x(k)$ and $y(k)$, $k = 0, 1, \ldots, N - 1$, denote the lth and mth rows of a Frank code matrix, where

$$\begin{aligned} x(k) &= e^{j2\pi\frac{kl}{N}}, \\ y(k) &= e^{j2\pi\frac{km}{N}}. \end{aligned} \tag{B2}$$

The cross correlation function between rows l and m, $C_{lm}(n)$, where $l = 0, 1, \cdots, N - 1$ and $m \equiv (l + r)\text{mod}N$ is given by

$$\begin{aligned} C_{lm}(n) &= e^{j2\pi\frac{nm}{N}} \sum_{k=0}^{N+n-1} e^{j2\pi\frac{k(l-m)}{N}}, \qquad \text{for} \quad n \leq 0, \\ C_{lm}(n) &= e^{j2\pi\frac{nl}{N}} \sum_{k=0}^{N-n-1} e^{j2\pi\frac{k(l-m)}{N}}, \qquad \text{for} \quad n > 0. \end{aligned} \tag{B3}$$

For $m \equiv (l + r) \bmod N$,

$$C_{lm}(n) = e^{j2\pi\frac{n(l+r)}{N}} \sum_{k=0}^{N+n-1} e^{-j2\pi\frac{kr}{N}}, \quad \text{for} \quad n \leq 0,$$
$$C_{lm}(n) = e^{j2\pi\frac{nl}{N}} \sum_{k=0}^{N-n-1} e^{-j2\pi\frac{kr}{N}}, \quad \text{for} \quad n > 0. \tag{B4}$$

From Eq. (B4) it is elementary to show that

$$\sum_{l=0}^{N-1} C_{lm}(n) = 0, \quad n = 0, \pm 1, \pm 2, \ldots, \pm(N-1) \quad \text{Q.E.D.} \tag{B5}$$

Appendix C

PROOF OF THEOREM 4

Theorem 4: For any coded sequence S_0, a subcomplementary set of sequences results from the Kronecker product of S_0 and a matrix consisting of a set of complementary sequences.

Proof: Consider the Kronecker product of any coded sequence S_0 and a complementary set of sequences that comprise the matrix B given by

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1N} \\ b_{21} & b_{22} & \cdots & b_{2N} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ b_{M1} & b_{M2} & \cdots & b_{MN} \end{bmatrix}. \tag{C1}$$

The Kronecker product of S_0 and B results in the ith row being

$$(b_{i1}S_0 \quad b_{i2}S_0 \quad b_{i3}S_0 \quad \cdots \quad b_{iN}S_0). \tag{C2}$$

Letting $X(t)$ denote the autocorrelation function of the L-element code S_0, the ACF of the sequence given by Eq. (C2), which we denote by $G_i(t)$, is easily shown to be

$$\begin{aligned} G_i(t) = {} & (b_{i1}\, b_{iN}^*)\, X\,(t) \\ & + (b_{i1}b_{i,N-1}^* + b_{i2}b_{iN}^*)\, X\,(t - L) \\ & + (b_{i1}b_{i,N-2}^* + b_{i2}b_{i,N-1}^* + b_{i3}b_{iN}^*)\, X\,(t - 2L) \\ & \cdot \\ & \cdot \\ & \cdot \\ & + (b_{i1}b_{i1}^* + b_{i2}b_{i2}^* + \cdots b_{iN}\, b_{iN}^*)\, X\,[(t - (N - 1)L] \\ & \cdot \\ & \cdot \\ & \cdot \\ & + (b_{i1}^*\, b_N)\, X\,[t - 2(N - 1)L]. \end{aligned} \tag{C3}$$

From Eq. (C3) it is observed that the coefficients of the $X(\cdot)$ terms are exactly the same as the ACF of the ith row of the complementary matrix B. Hence, it follows from the property of complementary sequences that

$$\sum_{i=1}^{M} G_i(t) = NM\, X\,[t - (N - 1)L]. \tag{C4}$$

Appendix D

DERIVATION OF THE P4/CHU CODE

In this appendix, we derive the Chu code [D1] by using the concept of integer functions. Chu stated this code without a derivation, then showed that it had periodic sidelobes equal to 0. The Lewis-Kretschmer P4 code (8) and its permutation set (see III E3) are the same as the Chu code except for a linear phase shift that does not affect the magnitude of the periodic or aperiodic autocorrelation function. Consider the $N \times N$ circulant matrix, A, associated with a periodic code. Let the first-row elements have the following form:

$$a_n = W_n^{f(n)}, \quad n = 0, 1, 2, \cdots, N-1 \tag{D1}$$

where $f(\cdot)$ is some real function of the integer n and

$$W_N = e^{-j\frac{2\pi}{N}}. \tag{D2}$$

Note that $W_N^N = 1$. We assume the following constraint equation (congruence) on $f(\cdot)$:

$$f(n) \equiv f(n + N) \bmod N. \tag{D3}$$

This congruence indicates the periodicity of f and implies that $f(n) - f(n + N)$ is an integer that is divisible by N.

The elements of the mth row of A can be written as

$$(W_N^{f(N-m+1)}, \ W_N^{f(N-m+2)}, \ \cdots, \ W_N^{f(2N-m)}), \tag{D4}$$

or using Eq. (D3) equivalently as

$$(W_N^{f(-m+1)}, \ W_N^{f(-m+2)}, \cdots, W_N^{f(-m+N)}). \tag{D5}$$

If $\mathbf{a}_m$ is a vector of length N equal to the mth row, then the condition that the code be perfect is

$$\mathbf{a}_i \mathbf{a}_j^t = 0, \quad i \neq j, \quad i, j = 1, 2, \cdots, N, \tag{D6}$$

where t is the conjugate transpose operation. Note that Eq. (D6) is representative of $(N-1)N/2$ equations. However, because of the rows are rotations of one another, only $N-1$ equations are not redundant. These distinct equations can be written as

$$\mathbf{a}_1 \mathbf{a}_m^t = 0, \quad m \neq 1. \tag{D7}$$

From Eqs. (D5) and (D7), we can show that the $N - 1$ nonredundant equations are

$$\sum_{n=0}^{N-1} W_N^{f(n)-f(n-m)} = 0; \qquad m = 1, 2, \cdots, N-1. \tag{D8}$$

We know that if

$$f(n) - f(n - m) = Mnm + g(m), \tag{D9}$$

where $g(m)$ is some integer function of n, and M is an arbitrary integer relatively prime to N, then Eq. (D8) is satisfied for all m. We seek the functional form of $f(n)$.

We let $f(n)$ be a polynomial of order L:

$$f(n) = \sum_{l=0}^{L} c_l n^l, \tag{D10}$$

where the c_l are to be determined. It is elementary to show that for $f(n)$ having the form given by Eq. (D10) that in order to satisfy Eq. (D9),

$$c_l = 0 \qquad \text{for} \quad l \geq 3. \tag{D11}$$

Hence $f(n)$ is a polynomial whose form is given by

$$f(n) = c_1 n + c_2 n^2. \tag{D12}$$

(Note that we have dropped the c_0 term since it is merely an arbitrary linear phase shift across all elements.) Now

$$\begin{aligned} f(n - m) &= c_1(n - m) + c_2(n - m)^2 \\ &= -2c_2 nm + c_1 n + c_2 n^2 - c_1 m + c_2 m^2. \end{aligned} \tag{D13}$$

Hence, if we subtract Eq. (D13) from Eq. (D12) and use the condition given by Eq. (D9), we find that

$$c_2 = \frac{1}{2} M, \tag{D14}$$

$$g(m) = c_1 m - c_2 m^2.$$

As a result,

$$f(n) = c_1 n + \frac{1}{2} M n^2. \tag{D15}$$

The form of c_1 can be determined from constraint congruence (Eq. (D3)). After substituting the functional form of $f(\cdot)$ as given by Eq. (D15) into Eq. (D3) and simplifying, we find that

$$\frac{1}{2}MN^2 + c_1N \equiv 0 \bmod N. \tag{D17}$$

It is required that the expression on the left of this congruence be an integer and divisible by N. It is easy to show that

- For N even, $c_1 = I$, arbitrary integer,
- For N odd, M even, $c_1 = I$,
- For N odd, M odd, $c_1 = I + \frac{1}{2}$.

Hence we can write

$$f(n) = \frac{1}{2}Mn^2 + \left[I + \frac{1}{2}[MN \bmod 2]\right]n. \tag{D18}$$

If we drop the arbitrary linear phase shift across all elements, it can be shown that an equivalent form is given by the expression

$$f(n) = \frac{1}{2}Mn(n + N \bmod 2). \tag{D19}$$

The P4 code (8) and its permutation set is the same as this code, which we call a P4/Chu code, except for a linear phase shift.

REFERENCE

D1. D.C. Chu, "Polyphase with Good Periodic Correlation Properties," *IEEE Trans. Inf. Theory* **18**, 531-532 (1972).

Appendix E

PROOF OF THE ROTATIONAL INVARIANCE OF THE APERIODIC ACF OF THE P4/CHU CODE

The proof for the rotational invariance of the P4 code is shown here in terms of the more general P4/Chu code described in Appendix D. The general form of the P4/Chu code as given by Eqs. (D1) and (D19) is

$$a_n = W_N^{(1/2)Mn(n+N \bmod 2)}, \qquad n = 0, 1, \cdots, N-1 \tag{E1}$$

where

W_N = $e^{-j\frac{2\pi}{N}}$,

M is an integer relatively prime to N, i.e., $(M, N) = 1$,

$N \bmod 2$ = $\begin{cases} 0 & \text{if } N \text{ even,} \\ 1 & \text{if } N \text{ odd.} \end{cases}$

An arbitrary rotation of this code that forms a new code is given by

$$a_n^{(k)} = W_N^{(1/2)M(n+k)(n+k+N \bmod 2)} \quad ; \quad \begin{matrix} n = 0, \cdots, N-1 \\ k = 0, 1, \cdots, N-1 \end{matrix} \tag{E2}$$

where k indexes the shifts in the rotation. We define a code word $\mathbf{a}^{(k)}$ of length N as

$$\mathbf{a}^{(k)} = (a_0^{(k)}, a_1^{(k)}, \cdots, a_{N-1}^{(k)}). \tag{3}$$

The aperiodic ACF sequence is defined as a vector $\mathbf{r}^{(k)}$ of length $2N - 1$:

$$\mathbf{r}^{(k)} = \mathbf{a}^{(k)} * \tilde{\mathbf{a}}^{(k)} = (r_{-(N-1)}^{(k)}, r_{-(N-2)}^{(k)}, \cdots, r_0^{(k)}, r_1^{(k)}, \cdots, r_{N-1}^{(k)}), \tag{E4}$$

where $*$ denotes linear convolution and $\sim$ denotes the time reversal complex conjugate of $\mathbf{a}$. We can show that

$$r_m^{(k)} = \sum_{n=0}^{N-1-m} a_n^{(k)} a_{n+m}^{(k)*}, \qquad m = 0, 1, 2, \cdots, N-1 \tag{E5}$$

and

$$r_{-m}^{(k)} = r_m^{(k)*}. \tag{E6}$$

We show that $|r_m^{(k)}|^2$ is independent of k or equivalently that the ACF of the P4/Chu code is invariant with rotation.

To this end, we substitute Eq. (E2) in Eq. (E5):

$$r_m^{(k)} = \sum_{n=0}^{N-1-m} W_N^{(1/2)M(n+k)(n+k+N \bmod 2)} W_N^{-(1/2)M(n+k+m)(n+k+m+N \bmod 2)}. \tag{E7}$$

Now

$$M(n + k)(n + k + N \bmod 2) - M(n + k + m)(n + k + m + N \bmod 2)$$

$$= -2Mkm - Mm^2 - Mm - Mm(N \bmod 2) - 2Mmn .$$

Thus

$$r_m^{(k)} = W_N^{-(1/2)M(2km+m^2+m+m(N \bmod 2))} \sum_{n=0}^{N-1-m} W_N^{-Mmn}, \qquad m = 0, 1, \cdots, N - 1. \tag{E8}$$

We see from Eq. (E8) that

$$|r_m^{(k)}|^2 = |\sum_{n=0}^{N-1-m} W_N^{-Mmn}|^2. \tag{E9}$$

Hence the magnitude of the ACF is independent of k or invariant with rotations of the original code.

Appendix F

PROOF OF THEOREM 5

Theorem 5: Consider an $N \times N$ matrix, E with elements on the unit circle. Let E have mutually orthogonal rows. In addition, let all rotations of any two columns of E be mutually orthogonal. Then a perfect periodic code results from concatenating the rows of E.

Proof: We define $\mathbf{c}_{nm}$ to be a vector equal to the nth column of E where this column has been circularly rotated m times. To be a perfect periodic code, we require that the $(N^2 \times N^2)$ circulant matrix T, whose first row is formed by concatenating the rows of E, have mutually orthogonal rows. The matrix T is given by

$$T = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1N} & e_{21} & \cdots & e_{N1} & \cdots & e_{NN} \\ e_{NN} & e_{11} & \cdots & e_{1,N-1} & e_{1N} & \cdots & e_{N-1,N} & \cdots & e_{N,N-1} \\ \cdot & & & & & & & & \\ \cdot & & & & & & & & \\ \cdot & & & & & & & & \\ e_{12} & e_{13} & \cdots & e_{21} & e_{22} & \cdots & e_{N2} & \cdots & e_{1} \end{bmatrix}. \tag{F1}$$

The inner product between rows i and j depends only on $i - j$. We denote the inner product between row 1 and row $m+1$ by r_m and require that r_m be equal to 0 for all m not equal to zero.

For $m \equiv 0 \ mod \ N$, because the rows are mutually orthogonal, $r_m = 0$. For $m \not\equiv 0 \ mod \ N$, it is straightforward to show that

$$\begin{aligned} r_1 &= (\mathbf{c}_{10},\mathbf{c}_{N1}) + (\mathbf{c}_{20},\mathbf{c}_{10}) + (\mathbf{c}_{30},\mathbf{c}_{20}) + \ldots + (\mathbf{c}_{N0},\mathbf{c}_{N-1,0}) \\ r_2 &= (\mathbf{c}_{10},\mathbf{c}_{N-1,1}) + (\mathbf{c}_{20},\mathbf{c}_{N1}) + (\mathbf{c}_{30},\mathbf{c}_{10}) + \ldots + (\mathbf{c}_{N0},\mathbf{c}_{N-2,0}) \\ &\cdot \\ &\cdot \\ &\cdot \\ r_{N^2-1} &= (\mathbf{c}_{10},\mathbf{c}_{2N}) + (\mathbf{c}_{20},\mathbf{c}_{3N}) + (\mathbf{c}_{30},\mathbf{c}_{4N}) + \ldots + (\mathbf{c}_{N0}\mathbf{c}_{1,N-1}), \end{aligned} \tag{F2}$$

where $(\cdot,\cdot)$ denotes the inner product of two vectors. For any inner product term $(c_{n_1 m_2}, c_{k_1 k_2})$ given in Eq. (F2), $n_1 \neq k_1$. Hence, if all rotations of any two columns of E are mutually orthogonal, it follows by inspection of Eq. (F2) that $r_n = 0$. Thus the theorem follows.

Appendix G

PROOF THAT FRANK-P4 PRODUCT CODE IS A PERFECT PERIODIC CODE

The Frank code of length N^2 is defined

$$a(n) = W_N^{n[n/N]}, \qquad n = 0, 1, \cdots, N^2 - 1 \tag{G1}$$

where

$$W_N = e^{-j(2\pi/N)}, \tag{G2}$$

and $[\cdot]$ is the least integer function.

The P4 code of length N^2, where N is odd, is defined

$$b(n) = W_{N^2}^{(1/2)Mn(n+1)}, \qquad n = 0, 1, \cdots, N^2 - 1 \tag{G3}$$

where M is relatively prime to N.

We form a new code called the Frank-P4 product code as follows:

$$c(n) = W_{N^2}^{(1/2)Mn(m+1)} \cdot W_N^{n[n/N]}, \qquad n = 0, 1, \cdots, N^2 - 1. \tag{G4}$$

We can show that $c(n)$ has zero sidelobes when implemented as a periodic code if $M + 1$ is also relatively prime to N. To this end, by using Eq. (G4) it can be shown that the periodic ACF of $c(n)$ is given by

$$r(k) = \sum_{n=0}^{N^2-1} W_N^{(n+k)[(n+k)/N]} W_{N^2}^{(1/2)M(n+k)(n+k+1)} W_N^{-n[n/k]} W_{N^2}^{(1/2)Mn(n+1)}, \tag{G5}$$

$$k = 1, 2, \cdots, N - 1.$$

We can show that Eq. (G5) reduces to

$$r(k) = W_{N^2}^{(k^2+k)M} \sum_{n=0}^{N^2-1} W_N^{(n+k)[(n+k)/N] - n[n/N]} W_{N^2}^{Mnk}, \tag{G6}$$

$$k = 1, 2, \cdots, N - 1.$$

Let

$$n = n_1 N + n_2, \tag{G7}$$

$$k = k_1 N + k_2, \tag{G8}$$

where $n_1, n_2, k_1, k_2 < N$. We rewrite Eq. (G6) as

$$r(k) = W_{N^2}^{(k^2+k)M} \sum_{n_2=0}^{N-1} \sum_{n_1=0}^{N-1} W_N^{(n_1N+n_2+k_1N+k_2)[(n_1N+n_2+k_1N+k_2)/N]-(n_1N+n_2)[(n_1N+n_2)/N]} W_{N^2}^{Mnk}. \tag{G9}$$

Simplifying Eq. (G9) gives

$$r(k) = W_{N^2}^{M(k^2+k)} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} W_N^{(n_2+k_2)(n_1+k_1)-n_2n_1} W_{N^2}^{Mnk}. \tag{G10}$$

Simplifying further yields

$$r(k) = W_{N^2}^{M(k^2+k)} W_N^{k_1k_2M} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} W_N^{n_2k_1+n_1k_2} W_{N^2}^{Mkn} \tag{G11}$$

$$= W_{N^2}^{M(k^2+k)} W_N^{Mk_1k_2} \sum_{n_1=0}^{N-1} \sum_{n_1=0}^{N-1} W_N^{n_2k_1+n_1k_2} W_{N^2}^{M(k_1N+k_2)(n_1N+n_2)}$$

$$= W_{N^2}^{M(k^2+k)} W_N^{Mk_1k_2} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} W_N^{n_2k_1+n_1k_2} W_N^{M(k_2n_1+k_1n_2)} W_{N^2}^{Mk_2n_1}$$

$$= W_{N^2}^{M(k^2+k)} W_N^{Mk_1k_2} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} W_N^{(M+1)n_2k_1} W_N^{(M+1)n_1k_2} W_{N^2}^{Mk_2n_2}$$

$$= W_{N^2}^{M(k^2+k)} W_N^{Mk_1k_2} \sum_{n_2=0}^{N-1} W_N^{(M+1)n_2k_1} W_{N^2}^{Mk_2n_2} \left[\sum_{n_1=0}^{N-1} W_N^{(M+1)k_2n_1} \right].$$

Now for $k_2 \neq 0$, and $M + 1$ relatively prime to N,

$$\sum_{n_1=0}^{N-1} W_N^{(M+1)k_2n_1} = 0. \tag{G12}$$

For $k_2 = 0$, $k_1 \neq 0$,

$$r(k) = r(k, N) = W_{N^2}^{M(k^2+k)} W_N^{Mk_1k_2} \sum_{n_2=0}^{N-1} N\, W_N^{(M+1)n_2k_1} = 0. \tag{G13}$$

Thus

$$r(k) = 0 \quad \text{for} \quad k = 1, 2, \cdots, N^2 - 1. \tag{G14}$$

Hence the Frank-P4 code is a perfect periodic code.

Appendix H

PERMUTATION CODES

Consider a perfect periodic code (PPC) word **a** with code elements a_n, $n = 0, 1, 2, \cdots, N-1$. Let $a_{N+n} = a_n$. Next, consider a periodic code **a'** with code elements a'_n, $n = 0, 1, \cdots, N-1$, where

$$a'_n = a_{Mn \bmod N} \tag{H1}$$

and M is relatively prime to N. We show that **a'** is also a PPC word. Define b_m such that

$$b_m = \sum_{n=0}^{N-1} a'_n a'^*_{n+m}. \tag{H2}$$

Now, **a'** is a PPC word if $b_m = 0$ for $m = 1, 2, \cdots, N-1$. We know that

$$a'_n = a_k, \; a'_{n+m} = a_{k+l} \tag{H3}$$

where there is a unique k and l for each n and m, respectively. If $m \neq 0$, then $l \neq 0$. Hence **a'** is perfect since

$$b_m = \sum_{n=0}^{N-1} a'_n a'^*_{n+m} = \sum_{k=0}^{N-1} a_k a^*_{k+l} = 0. \tag{H4}$$

Appendix I

INDEX CODES

Consider the following code with P elements:

$$W_k^{l\ \mathrm{ind}_\alpha(0)},\quad W_k^{l\ \mathrm{ind}_\alpha(1)},\quad W_k^{l\ \mathrm{ind}_\alpha(2)},\quad \cdots,\quad W_k^{l\ \mathrm{ind}_\alpha(P-1)}, \tag{I1}$$

where

P	is a prime integer,
α	is a primitive root of P,
$\mathrm{ind}_\alpha(\cdot)$	is the integer index function to the base α,
k	is a divisor of $P-1$, $1<k\le P-1$,
l	is integer not divisible by n,
W_k	$= e^{-j2\pi/k}$, and
$W_k^{l\ \mathrm{ind}_\alpha x}$	$= 0$ for $x = 0$.

We show that the periodic code given by Eq. (I1) has a constant sidelobe level -1.

We can show that the mth row of the circulant matrix A can be written as

$$W_k^{l\ \mathrm{ind}_\alpha(P+1-m)},\quad W_k^{l\ \mathrm{ind}_\alpha(P+1-m+1)},\quad \cdots,\quad W_k^{l\ \mathrm{ind}_\alpha(P+1-m+p-1)}. \tag{I2}$$

Let b_m be the inner product between the first row and the $m+1$th row, then

$$b_m = \sum_{n=0}^{b-1} W_k^{l\ \mathrm{ind}_\alpha n - l\ \mathrm{ind}_\alpha(n-m)},\qquad m = 1, 2, \cdots, P-1 \tag{I3}$$

where we have used the fact that $\mathrm{ind}_\alpha(P-m+n) = \mathrm{ind}_\alpha(n-m)$.

A theorem [I1] in number theory states that the expression given by Eq. (I3) under the conditions previously given for P, α, l and k is equal to -1. Hence

$$b_m = -1,\qquad m = 1, 2, \cdots, P-1 \tag{I4}$$

and the periodic code given by Eq. (I1) has a constant sidelobe level equal to -1.

REFERENCE

I1. I.M. Vinogradov, *Elements of Number Theory* (Dover Publications, 1954).